

1 DAVID H. HARPER*
david.harper@haynesboon.com
2 JASON P. BLOOM*
jason.bloom@haynesboone.com
3 **HAYNES AND BOONE, LLP**
2801 N. Harwood Street
4 Suite 2300
Dallas, Texas 75201
5 Telephone: (214) 651-5000
Facsimile: (214) 651-5940
6 *Admitted Pro Hac Vice

7 JASON T. LAO, SBN 288161
jason.lao@haynesboone.com
8 ANDREA LEVENSON, SBN 323926
andrea.levenson@haynesboone.com
9 **HAYNES AND BOONE, LLP**
600 Anton Boulevard, Suite 700
10 Costa Mesa, California 92626
Telephone: (949) 202-3000
11 Facsimile: (949) 202-3001

12 *Attorneys for Plaintiff*
13 *X Corp.*

14 **UNITED STATES DISTRICT COURT**
15 **NORTHERN DISTRICT OF CALIFORNIA**

16 X CORP., a Nevada corporation,
17 Plaintiff,
18 vs.
19 BRIGHT DATA LTD., an Israeli
20 corporation,
21 Defendant.

Case No. 3:23-cv-03698-WHA

FIRST AMENDED COMPLAINT
JURY TRIAL DEMAND

1 Plaintiff X Corp. (“X Corp.” or “Plaintiff”), by and through its undersigned counsel, hereby
2 files its First Amended Complaint against Defendant Bright Data Ltd., (“Bright Data” or
3 “Defendant”), and in support thereof alleges as follows:

4 **INTRODUCTION**

5 1. Defendant Bright Data Ltd. has built an illicit data-scraping business on the backs
6 of innovative technology companies like X Corp., which operates the social media platform
7 formerly known as Twitter and now known as X. Bright Data scrapes and sells millions of records
8 from X Corp.’s X platform, in blatant violation of X Corp.’s Terms of Service, by which Bright
9 Data is bound. Bright Data also induces and facilitates other X users to violate their own
10 agreements with X Corp. by selling automated data-scraping tools and services that specifically
11 target a wide range of X Corp. data.

12 2. Bright Data uses elaborate technical measures to evade X Corp.’s anti-scraping
13 technology, taxing the resources of X Corp.’s servers and hampering the user experience for
14 legitimate X users. Bright Data is aware that its activities violate X Corp.’s Terms because the
15 company and its executives are registered X account holders who have agreed to abide by those
16 Terms.

17 3. X Corp. brings this action for injunctive relief to halt Bright Data’s unauthorized
18 use of X Corp.’s platform and for damages caused by Bright Data’s breach.

19 **THE PARTIES**

20 4. Plaintiff X Corp. is a privately held corporation duly organized and existing under
21 the laws of the State of Nevada with its principal place of business at 1355 Market Street, Suite
22 900, San Francisco, California, 94103. X Corp. owns and operates the social media platform X,
23 formerly known as Twitter.

24 5. On information and belief, Defendant Bright Data was incorporated in Israel in
25 2008 as Zon Networks Ltd. and changed its name to Bright Data Ltd. in 2021. Bright Data has its
26 principal place of business at 4 Hamahshev St., Netanya 4250714, in Israel. Bright Data has at
27 times maintained an office at L415 Mission Street, 37th Floor, in San Francisco, California.

28 6. Defendant Bright Data operates brightdata.com, where it sells data scraped from

numerous websites and social media platforms, including X, along with tools and services to scrape data from X and other platforms.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under 28 U.S.C. § 1332 because complete diversity exists, and the amount in controversy exceeds \$75,000. Plaintiff X Corp. is incorporated in Nevada with its principal place of business in California. Defendant Bright Data is incorporated in Israel with its principal place of business in Israel.

8. This Court has personal jurisdiction over Defendant because Defendant has consented to X Corp.'s Terms, which require all disputes related to the Terms be brought in the federal or state courts located in San Francisco, California. As part of its agreement to those Terms, Defendant also consented to personal jurisdiction in California.

9. Additionally, this Court has personal jurisdiction over Defendant because Defendant knowingly directed prohibited conduct to California and California residents. Defendant offers its data sets and scraping tools for sale in California and to California residents, and has targeted X Corp., which has its principal place of business in California, as well as X Corp.'s users located in California.

10. Defendant markets and sells its products to California residents and businesses via a sales office in California, according to its website:

Figure 1: Screenshot of Bright Data's website on November 14, 2023



1 See Exh. A.

2 11. As recently as October 19, 2022, Defendant encouraged customers to contact Bright
3 Data at its California sales office, as shown in Figure 2.

4 **Figure 2: Screenshot from Bright Data’s “Contact Us” page on October 19, 2022**



18 See Exh. B.

19 12. Members of Defendant’s business development and sales team are also located in
20 California. For example, Defendant’s Chief Revenue Officer, who oversees Bright Data’s sales
21 operations, is based in the San Francisco Bay Area. See Exh. C. Defendant’s Global Head of
22 Presales is also based in California, along with numerous other Bright Data employees. See Exh.
23 C.

24 13. Defendant has also specifically targeted its products at the California market. For
25 instance, Defendant’s interactive website, through which California residents can purchase
26 Defendant’s scraping tools and scraped data sets, offers a “Superior California Proxy” product that
27 promises “[v]ast numbers of California IPs to get data off any website.”
28

Figure 3: Screenshot from Bright Data's website on November 14, 2023

See Exh. D. These proxy IP addresses are designed to evade usage restrictions and anti-scraping technology, such as those implemented by X. In fact, Defendant specifically advertises that its California proxies allow users to “[o]vercome all blocks all of the time in California.”

14. On information and belief, Defendant has sold its scraping tools, scraped data sets, and IP proxies to X users, including X users in California, and has scraped data from X Corp. servers in California.

15. Venue is proper in this district under 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to the claims occurred in this judicial district. During all relevant times, Defendant repeatedly, knowingly, and intentionally targeted its wrongful acts at X Corp., which has its principal place of business in this district. Defendant also, on information and belief, sold its scraping tools, scraped data sets, and IP Proxies to residents of this district, including through Defendant’s sales office located in this district and employees located in this district.

16. Pursuant to Civil L.R. 3-2(d), this case may be assigned to either the San Francisco or Oakland division because X Corp. is located in San Francisco County.

FACTUAL ALLEGATIONS

A. X Corp.'s Platform and Terms of Service

17. Plaintiff X Corp. owns and operates the social media platform X, accessible through twitter.com, X.com and various mobile and online applications.

18. The X platform has hundreds of millions of active users worldwide. More than 23 million X accounts have been registered from California.

19. X Corp. allows its registered users to post and share content, including written comments, images and videos, known as posts, and to share, like and comment on other users' posts.

20. To post content on X or to re-post, like or otherwise interact with posts by others, users must register for an account and log in to that account.

21. To register for an account, users must provide their name, phone number or email address, and date of birth. To prevent automated services from registering for accounts, X Corp. requires potential account holders to complete a "CAPTCHA" fraud-detection process to determine whether the user is human. X Corp. then verifies registrants through email or phone confirmation.

22. All users who register for a X account, and/or view the X website or application agree to a binding contract with X Corp. as outlined in X Corp.'s User Agreement, which is comprised of the Terms of Service, Privacy Policy, and the Rules and Policies (collectively the "Terms").

23. X Corp.'s Terms state that a user may not "access, tamper with, or use non-public areas of the Services, our computer systems, or the technical delivery systems of our providers" or "breach or circumvent any security or authorization measures."

24. X Corp.'s Terms also state a user may not "access or search or attempt to access or search the Services by any means (automated or otherwise) other than through our currently available, published interfaces that are provided by us (and only pursuant to the applicable terms and conditions), unless you have been specifically allowed to do so in a separate agreement with us."

1 25. In addition, X Corp.’s Terms specifically state that “crawling or scraping the
2 Services in any form, for any purpose without our prior written consent is expressly prohibited.”

3 26. Under the Terms, users may not “forge any TCP/IP packet header or any part of the
4 header information in any email or posting, or in any way use the Services to send altered,
5 deceptive or false source-identifying information.”

6 27. Users are also prohibited under the Terms from any conduct that would “interfere
7 with, or disrupt, (or attempt to do so), the access of any user, host or network, including ...
8 overloading, flooding, spamming ... or by scripting the creation of Content in such a manner as to
9 interfere with or create an undue burden on the Services.”

10 28. The Terms also incorporate by reference X Corp.’s Platform Manipulation and
11 Spam Policy (the “Policy”), which specifically prohibits “coordinated harmful activity that
12 encourages or promotes behavior which violates [X Corp.’s] Rules.” The Policy also prohibits
13 “leveraging X’s open source code to circumvent remediations or platform defenses.”

14 29. The Terms prohibit selling any content collected from the platform. Users may not
15 “reproduce, modify, create derivative works, distribute, sell, transfer, publicly display, publicly
16 perform, transmit, or otherwise use the Services or Content on the Services” unless otherwise
17 authorized by the Terms or a developer agreement.

18 30. The Terms also expressly state that it is “a violation of these Terms to facilitate or
19 assist others in violating these Terms, including by distributing products or services that enable or
20 encourage violation of these Terms.”

21 31. Advertisers on the X platform are also subject to X Corp.’s Ads Policies, which
22 expressly state that advertisers must follow the Terms and all X Corp. Rules.

23 32. For developers who wish to retrieve or analyze X Corp.’s data, X Corp. offers
24 specialized access to its Application Programming Interfaces (“APIs”) through a tiered
25 subscription service.

26 33. X Corp.’s Developer Agreement also limits the access of developers to X Corp.’s
27 content. The Agreement instructs developers that they may “not exceed or circumvent rate limits,
28 or any other limitations or restrictions described in this Policy or your agreement with Twitter,

1 listed on the Developer Site, or communicated to you by Twitter.”

2 **Background on Data Scraping**

3 34. Scraping is the process of using automated means to collect content or data from a
4 website. The process involves making a request to a website’s server, downloading the results and
5 parsing them to extract the desired data. Data scrapers typically send large volumes of these
6 requests, taxing the capacity of servers and diminishing the experience for legitimate users.

7 35. X Corp. utilizes a variety of technological measures to detect and prevent
8 automated systems from scraping data from its platform, including industry standard automation
9 prevention techniques, such as CAPTCHAs, user identification and IP rate limits and anomaly
10 detection tools.

11 36. X Corp.’s registration process requires potential registrants to pass a CAPTCHA
12 and provide a valid phone number or email address. Prior to creating the user’s account, X Corp.
13 sends a verification code to the email or phone number. Potential users must enter the verification
14 code to create an account.

15 37. X Corp. also employs rate limits that cap the number of posts that may be viewed
16 by registered users and those who access the platform without an account. Developers who use the
17 X API are also capped in the number of posts they may post to, or pull from, the platform based
18 on their subscription level.

19 38. X Corp. also utilizes anomaly detection to detect and block automated software that
20 is attempting to access X Corp.’s platform.

21 **Defendant Has Agreed to X Corp.’s Terms of Service**

22 39. Defendant has expressly agreed to X Corp.’s Terms and is therefore bound by those
23 Terms.

24 40. Initially, by using the X platform, Defendant, which is well aware of the Terms,
25 agrees to be bound by them. The Terms specifically state:

26 These Terms of Service (“Terms”) govern your access to and use of our services,
27 including our various websites, SMS, APIs, email notifications, applications,
28 buttons, widgets, ads, commerce services, and our other covered services
(<https://help.x.com/rules-and-policies/x-services-and-corporate-affiliates>) that link
to these Terms (collectively, the “Services”), and any information, text, links,
graphics, photos, audio, videos, or other materials or arrangements of materials

uploaded, downloaded or appearing on the Services (collectively referred to as “Content”). By using the Services you agree to be bound by these Terms.

41. In addition to agreeing to the Terms by using X services, Defendant, which has maintained a registered account on X (@bright_data) since at least February 2016, expressly accepted and agreed to the Terms when registering its account. Bright Data’s X account frequently posts content promoting the company’s products and services.

42. Defendant’s top executives are also registered X users and expressly agreed to X Corp.’s Terms when registering their accounts, further demonstrating that Bright Data had knowledge of the Terms:

- a. Bright Data’s CEO, Or Lenchner, has maintained a registered account on X (@orlench) since at least December 2012 and regularly posts from that account.
- b. Bright Data’s CMO, Yanay Sela, has maintained a registered X account (@yanay_sela) since at least December 2014.
- c. Bright Data’s Managing Director for North America, Omri Orgad, has maintained a registered X account (@omri_orgad) since at least November 2011.
- d. Bright Data’s Vice President of Product, Erez Naveh, has maintained a registered X account (@nerez) since at least August 2009.
- e. Bright Data’s Global Communications Manager, Zachary Keyser, has maintained a registered X account (@KeyserZachary) since at least December 2019.
- f. Bright Data’s Founder, Ofer Vilenski, has maintained a registered X account (@vilenski) since at least November 2008.

43. On information and belief, several other employees and agents of Defendant involved in Defendant’s data-scraping activities are also X account holders, including, by way of example, Artem Shibakov, a Bright Data software engineer who has maintained a registered X account (@ashibakow) since at least February 2013. These account holders have also expressly accepted and agreed to X Corp.’s Terms.

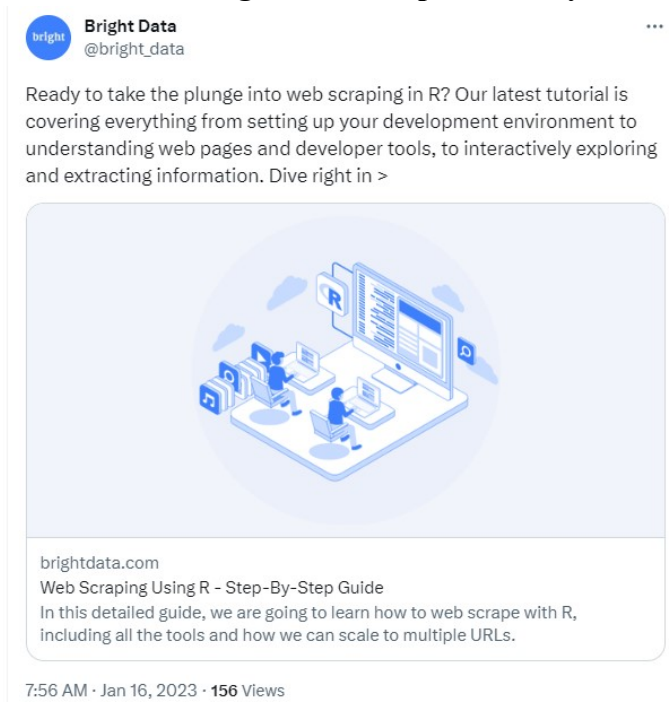
44. Defendant is additionally subject to the Terms as an advertiser on X. Beginning on March 7, 2016, Defendant (then known as Luminati Networks) purchased advertising on the X platform. Defendant purchased additional advertising on X from 2019 to 2021. As stated in X

1 Corp.'s Ad Policies, to which Defendant expressly agreed, all advertisers are bound by the
2 platform's Terms and Rules.

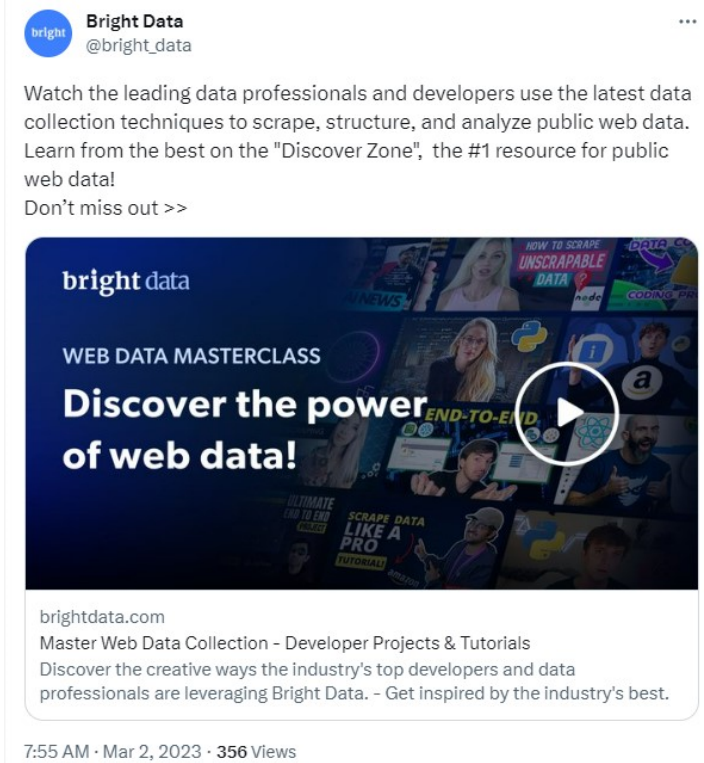
3 45. Defendant and its executives have repeatedly used these X accounts to discuss and
4 promote their data-scraping products and services, including but not limited to the following posts:

- 5 a. On January 1, 2023, Defendant posted a video on X entitled "How to Scrape
6 UNSCRAPABLE data!" which demonstrated how to use Defendant's tools and
7 services for unauthorized data scraping.
- 8 b. On January 16, 2023, Defendant encouraged users in a post on X to "take the plunge
9 into web scraping" using a "step-by-step guide" to Defendant's tools and services.

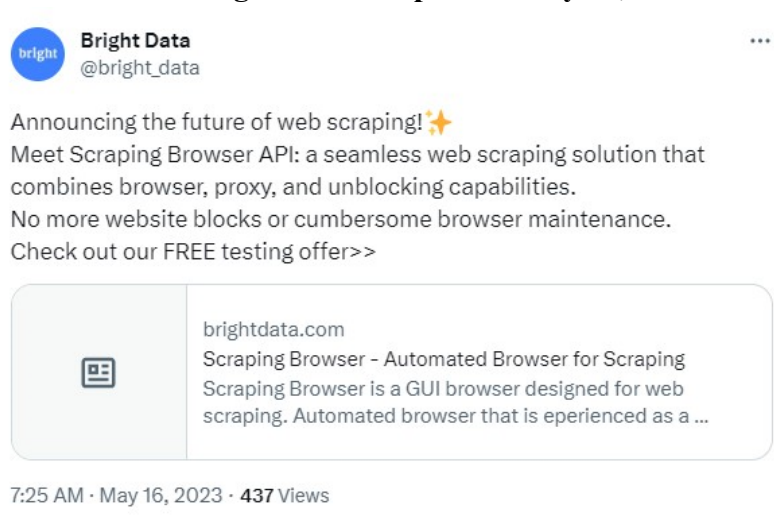
10 **Figure 4: Screenshot of Bright Data's X post on July 11, 2023**



- 22 c. On March 2, 2023, Defendant posted a video on X to a "masterclass" that showed
23 "the latest data collection techniques to scrape, structure, and analyze public web
24 data" using Defendant's tools and services.

Figure 5: Screenshot of Bright Data's X post on July 11, 2023

- d. On March 23, 2023, Defendant posted a promoted its "Web Unblocker" and its ability to "bypass[] multiple anti-bot solutions" in a post on X.
- e. On May 16, 2023, Defendant promoted its "Scraping Browser API: a seamless web scraping solution that combines browser, proxy, and unblocking capabilities" with a link to a "FREE testing offer" in a post on X.

Figure 6: Screenshot of Bright Data's X post on July 11, 2023

Defendant's Unauthorized Scraping

46. Defendant, per its own admissions, has engaged in widespread scraping of X Corp.'s data, circumventing X Corp.'s technical barriers and violating the Terms to which it agreed. Defendant has also facilitated the scraping of data from X and induced X users to violate X Corp.'s Terms.

47. X Corp. has not granted Defendant permission to scrape data from the X platform.

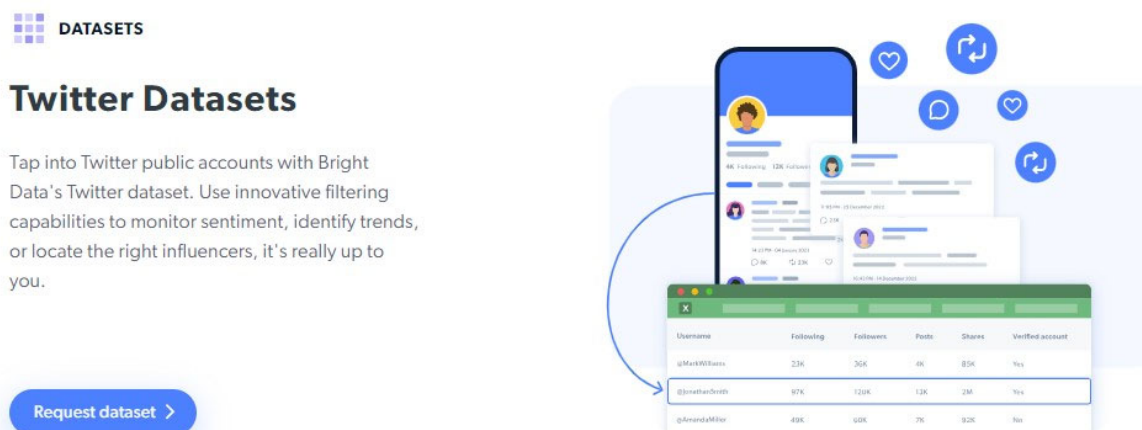
48. X Corp permits paying customers to lawfully access certain categories of X data, subject to contractual usage limits and other restrictions designed to protect the X platform and user experience. Rather than attempt to lawfully acquire X data through authorized means, Bright Data elected to scrape the data (and enable others to do so), using proxies and other illicit methods to shield its identity and scraping activities.

49. Defendant has not publicly disclosed how it evades X Corp.'s technical safeguards against scraping. However, Defendant's website makes clear that the company engages in prohibited scraping on an industrial scale and brazenly advertises that Defendant sells tools and services that encourage and enable others to engage in prohibited scraping.

Defendant Scrapes and Sells X Corp. Data

50. As seen in Figure 7 below, Defendant offers X Corp.'s data for sale on its website.

Figure 7: Screenshot of Bright Data's website on July 10, 2023

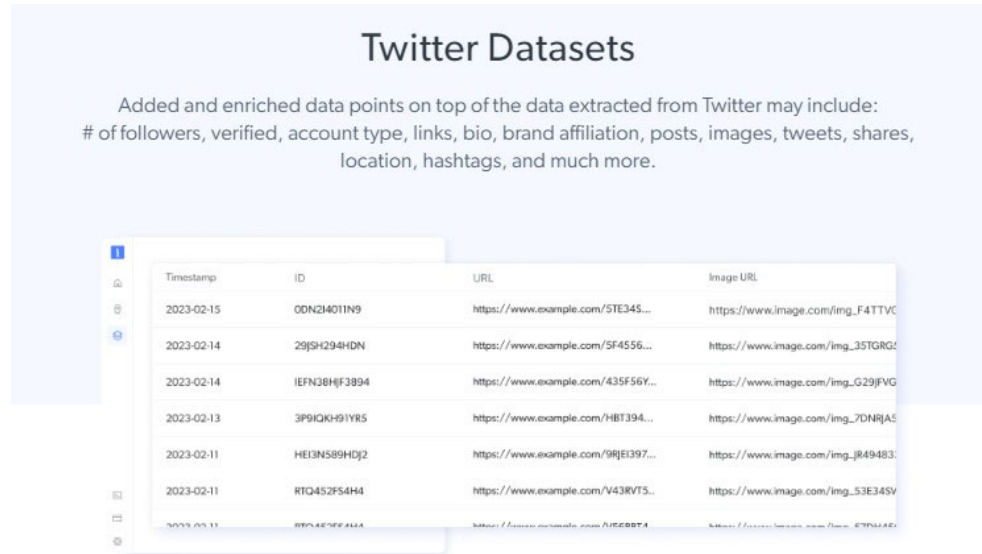


See Exh. E.

51. According to Defendant's website, the X Corp. data sets offered for sale by

Defendant include “millions of pages and tens of millions of data points.” Specifically, these data sets include the following user information: “# of followers, verified, account type, links, bio, brand affiliation, posts, images, tweets, shares, location, hashtags, and much more.”

Figure 8: Screenshot of Bright Data’s website on July 10, 2023



See id.

52. Defendant could have only obtained this data by engaging in prohibited scraping of X’s platform.

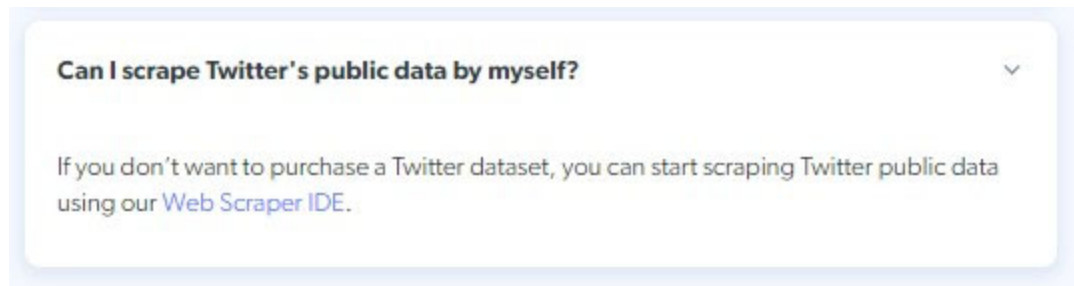
53. Defendant offers this unlawfully obtained data for sale starting at \$.01 per record, but also offers customized packages of X Corp.’s data.

54. Defendant also offers several options for delivery of X Corp.’s data, and even offers its customers the opportunity to regularly update its data sets with additional data scraped from X at regular intervals.

Bright Data Sells Automated Tools to Scrape X Corp.’s Data

55. Defendant also offers for sale on its website automation software that allows users to scrape data directly from the X platform in violation of X Corp.’s Terms.

56. As indicated in Exhibit F, Defendant’s website states: “If you don’t want to purchase a Twitter dataset, you can start scraping Twitter public data using our Web Scraper IDE.”

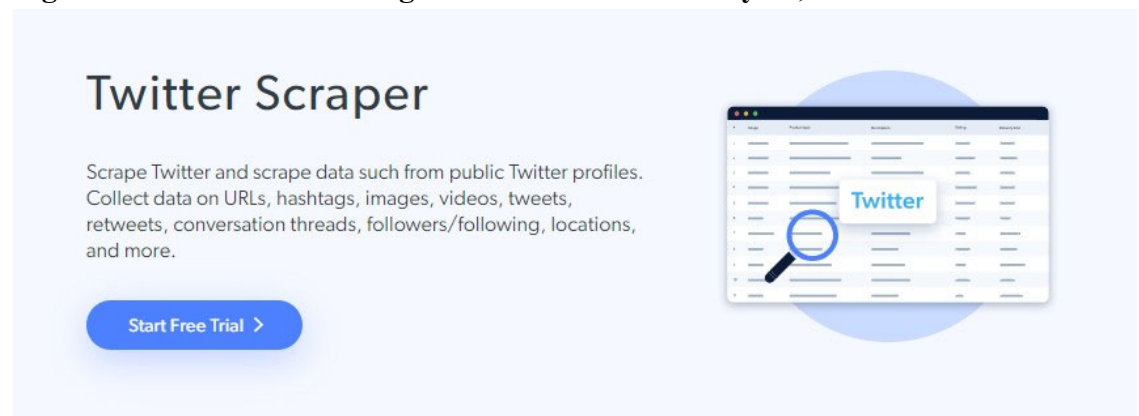
Figure 9: Screenshot of Bright Data's website on July 10, 2023

See Exh. E.

57. Defendant's Web Scraper tool allows individuals to evade detection utilizing a proxy network in order "to remain anonymous, avoid IP blocking, access geo-restricted content, and improve scraping speed." The tool also includes an "unblocking solution" that is designed to evade anti-scraping measures like those employed by X Corp. Defendant specifically advertises that its Web Scraper tool can be used to "[e]asily scrape data from any geo-location while avoiding CAPTCHAs and blocks."

58. In addition to its Web Scraper tool, Defendant sells at least four additional tools designed to scrape information specifically from the X Platform: Twitter Scraper, Twitter Profile Scraper, Twitter Image Scraper, and Twitter Followers Scraper.

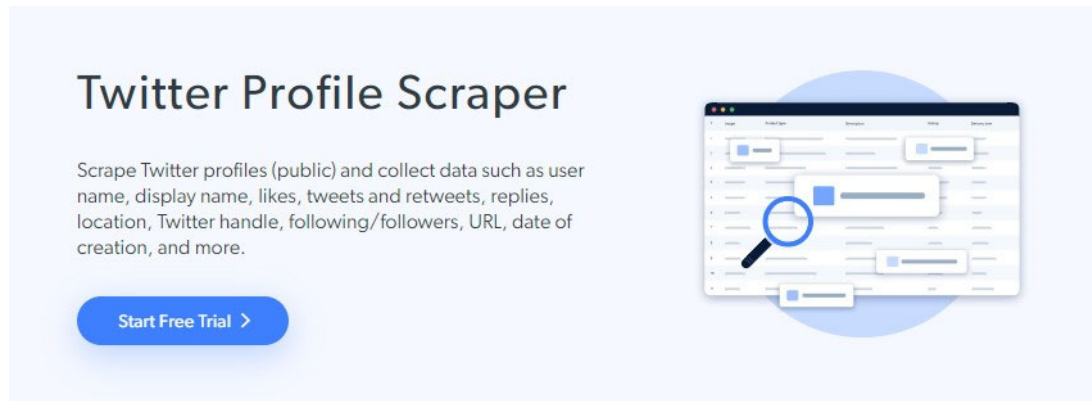
- a. As seen in Figure 7 below, Defendant offers a Twitter Scraper to automatically scrape data from the X platform, including "URLs, hashtags, images, videos, tweets, retweets, conversation threads, followers/following, locations, and more."

Figure 10: Screenshot of Bright Data's website on July 10, 2023

See Exh. F.

- b. As seen in Figure 11 below, Defendant offers a Twitter Profile Scraper to automatically “collect data such as user name, display name, likes, tweets and retweets, replies, location, Twitter handle, following/followers, URL, date of creation, and more.”

Figure 11: Screenshot of Bright Data’s website on July 10, 2023



See Exh. G.

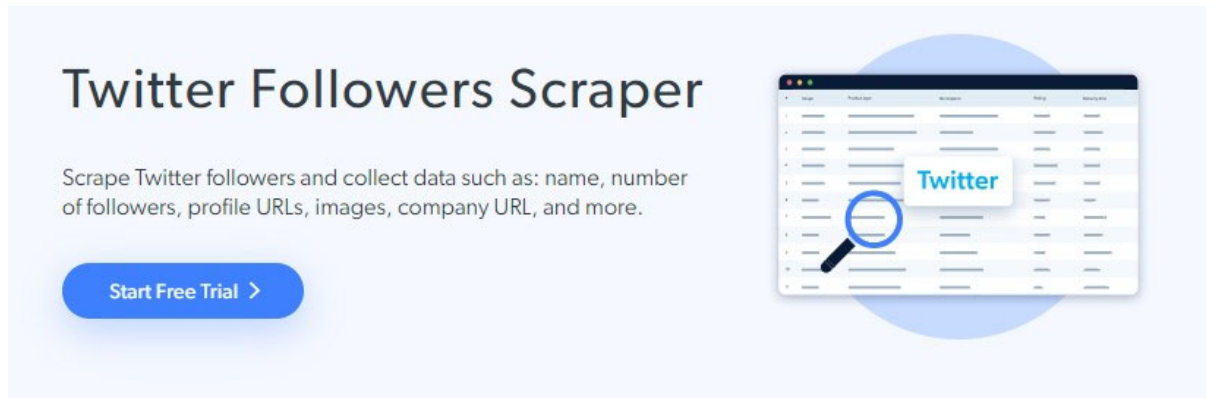
- c. As seen in Figure 12 below, Defendant also offers a Twitter Image Scraper to automatically “collect data such as user name, Twitter handle, following/followers, location, URL, date of creation, and more.”

Figure 12: Screenshot of Bright Data’s website on July 10, 2023



See Exh. H.

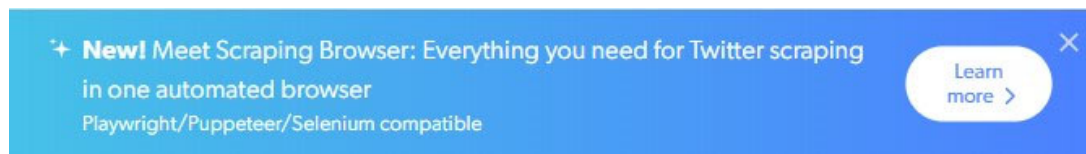
- d. As seen in Figure 13 below, Defendant has also offered a Twitter Followers Scraper to automatically collect data such as “name, number of followers, profile URLs, images, company URL, and more.”

Figure 13: Screenshot of Bright Data’s website on July 10, 2023

See Exh. I.

59. For each of these products, Defendant claims it “[u]tilizes proprietary technology to unlock sites” and allows customers to “collect as much data as you need quickly and completely.”

60. In addition to these X-specific scraping tools, Bright Data offers an automated “Scraping Browser” that simplifies the act of scraping data from the X platform. As seen in Figure 14 below, Bright Data markets this product for scraping X Corp.’s data.

Figure 14: Screenshot of Bright Data’s website on July 10, 2023

See Exh. G.

61. Defendant advertises this “Scraping Browser” as containing “all website unlocking operations under the hood, including: CAPTCHA solving, browser fingerprinting, automatic retries, selecting headers, cookies, & Javascript rendering, and more.” Defendant also claims its Scraping Browser “automatically learns to bypass bot-detection systems as they adapt, saving you the hassle and cost.”

62. The Scraping Browser allows Defendant’s customers to “appear as a real user browser to bot-detection system[s],” such as those used by X Corp.

Bright Data Sells Proxy Services to Facilitate Data-Scraping

63. Defendant also facilitates the violation of X Corp.’s Terms by offering proxy services specifically designed to evade anti-scraping measures, including X Corp.’s CAPTCHAs and its user ID and IP rate limits. These tools impersonate actual X users in order to bypass X Corp.’s defenses.

64. These proxy services imitate requests from legitimate users in order to conceal the true requestor’s IP address and location. Defendant advertises that these proxies will “avoid[] IP bans and CAPTCHAs” and allow users to “[g]ather vast amounts of public web data with total anonymity.” *See* Exh. J.

FIRST CAUSE OF ACTION

(Breach of Contract)

65. X Corp. realleges and incorporates all preceding paragraphs herein.

66. Use of the X platform and use of X Corp.’s services are governed by X Corp.’s Terms.

67. X users, including Defendant, accept the Terms as a condition of using the platform.

68. Moreover, by virtue of having X accounts, Defendant has expressly accepted and agreed to X Corp.’s Terms.

69. The Terms are enforceable and binding on Defendant.

70. Defendant has repeatedly violated the Terms, including by (i) accessing the X platform through automated means without specific authorization from X Corp.; (ii) scraping data from the X platform without authorization; (iii) selling tools that enable others, including X users, to access the X platform by automated means and to scrape data; (iv) selling proxy services that enable others, including X users, to access the X platform by automated means and evade X Corp.’s anti-automation and anti-scraping tools; and (v) selling data that Defendant scraped from the X platform.

71. Defendant has breached and continues to breach the Terms by scraping data from X Corp.’s platform without prior consent from X Corp. X Corp. has never authorized Defendant to access its platform through automated means and has never given Defendant consent to scrape

1 data.

2 72. Despite being bound by the Terms, Defendant has repeatedly accessed the X Corp.
3 platform through automated means and scraped data in violation of the Terms.

4 73. Defendant has breached, and continues to breach, X Corp.'s Terms by accessing
5 the platform through unauthorized means and scraping data from the platform.

6 74. Defendant has breached, and continues to breach, X Corp.'s Terms by selling tools
7 that allow other X users to access the platform by automated means and scrape data, and by selling
8 proxy services that allow the same.

9 75. Defendant has breached, and continues to breach, X Corp.'s Terms by selling data
10 that Defendant has scraped from X Corp.'s platform.

11 76. Defendant's conduct has damaged X Corp. and caused and continues to cause
12 irreparable harm and injury to X Corp.

13 77. X Corp. is entitled to compensatory damages, injunctive relief, declaratory relief,
14 and/or other equitable relief.

15 **SECOND CAUSE OF ACTION**

16 (Tortious Interference with Contract)

17 78. X Corp. realleges and incorporates all preceding paragraphs herein.

18 79. All X users must agree to abide by the Terms, which constitute a valid and
19 enforceable agreement between X Corp. and each user.

20 80. As a user of X Corp.'s platform, as well as a present or former X account holder,
21 Defendant is aware of the Terms and that they govern all users who choose to interact with the X
22 platform. Defendant is also aware of the Terms because several of its executives and employees
23 are present or former X account holders.

24 81. Nevertheless, Defendant has marketed and sold its scraping tools to X users and
25 account holders, including X users and account holders residing in California, through its
26 interactive website accessible in California and elsewhere, through its sales office and employees
27 in California and elsewhere, and by using the X platform to market its scraping services to other
28 X users and account holders.

1 and disgorgement of Defendants' profits in an amount to be determined at trial, compensatory
2 damages, injunctive relief, declaratory relief, and/or other equitable relief.

3 **FOURTH CAUSE OF ACTION**

4 (Trespass to Chattels)

5 94. X realleges and incorporates all preceding paragraphs herein.

6 95. The X platform and all underlying technological infrastructure are the personal
7 property of X Corp.

8 96. Defendant intentionally entered into, and made use of, X Corp.'s technological
9 infrastructure, including its software and servers located in California, to obtain information for its
10 own economic benefit.

11 97. Defendant knowingly exceeded the permission granted by X Corp. to access its
12 personal property, including its technological infrastructure and servers.

13 98. Defendant's acts have diminished the server capacity that X Corp. can devote to its
14 legitimate users, and thereby injured X Corp. by depriving it of the ability to use its personal
15 property.

16 99. Through its acts, Defendant also caused other persons, including X users and
17 account holders based in California and elsewhere, to knowingly exceed the permission granted
18 by X Corp. to access its personal property, further injuring X Corp.

19 100. X Corp. has never consented to Defendant's conduct.

20 101. Defendant's conduct constitutes trespass to X Corp.'s chattels.

21 102. Defendant's acts have caused injury to X Corp. and if continued, expanded, and/or
22 replicated unchecked by others, will cause damage in the form of impaired condition, quality, and
23 value of its servers, technology infrastructure, services, and reputation.

24 **FIFTH CAUSE OF ACTION**

25 (Unlawful, Unfair or Fraudulent Business Practices (Cal. Bus. & Prof. Code § 17200 et seq.))

26 103. X Corp. realleges and incorporates all preceding paragraphs herein.

27 104. Defendant's actions described above constitute unlawful, unfair, or fraudulent acts
28 or practices in the conduct of a business, in violation of California's Business and Professions

Code Section 17200, et seq, including because they constitute trespass and tortious interference with business relationships in violation of the law, and because Defendant deceived X Corp. into providing it access to, and information from, the X Corp. computer network. Defendant's data-collection technology and its data-scraping tools deliberately misrepresented the requests sent to the X platform, posing as legitimate X users, and Defendant's sale of IP proxies masquerades as a legitimate X user to avoid X Corp.'s technical measures designed to prevent unauthorized access of its computer servers.

105. Scraping data, as well as circumventing X Corp.'s ability to police its own platform, has caused substantial injury to X Corp., in the form of costs to investigate, remediate, and prevent Defendant's wrongful conduct, among other injuries.

106. As a result of Defendant's various acts and omissions, X Corp. has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendant's actions are enjoined.

SIXTH CAUSE OF ACTION

(Misappropriation)

107. X Corp. realleges and incorporates all preceding paragraphs herein.

108. X Corp. has invested substantial time, labor, skill, and financial resources into the creation and maintenance of X, its computer systems, and servers, including system and server capacity, as well as the content on X. Defendant has not invested any of its own time nor resources to the development of the X platform.

109. Defendant used automated means—in violation of X Corp.'s Terms—to wrongfully access the X platform, systems and servers, including systems and servers located in California, and obtain data from the X platform.

110. Defendant appropriated this data at little or no cost to Defendant, free-riding on X Corp.'s substantial investment of time, effort and expense.

111. As a result of Defendant's misappropriation, X Corp. has been forced to expend additional time, labor, skill and financial resources to investigate and mitigate Defendant's wrongful conduct. Defendant has been able to exploit and profit from X Corp.'s substantial

investments in the X platform.

112. X Corp. has been and will continue to be damaged as a result of Defendant's misappropriation.

113. X Corp. has suffered and will continue to suffer irreparable injury, and its remedy at law is not itself adequate to compensate it for injuries inflicted by Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief, as follows:

1. Preliminary and permanent injunctive relief enjoining Bright Data, its agents, officers, employees and successors from:

- a. accessing or using X Corp.'s website, servers, systems, and any data contained therein for purposes of unlawful data scraping;
- b. developing or distributing any technology or product that is used, or could be used, for the unauthorized scraping of data from X;
- c. facilitating the scraping of data by other users;
- d. selling or offering for sale any data previously obtained from X;
- e. utilizing any proxies to access X's website, servers, systems, and any data contained therein; and
- f. selling or offering for sale any proxies that can be used to access X's website, servers, systems, and any data contained therein.

2. That Defendant be required to identify the location of any and all data obtained from the X platform and to destroy any and all such data;

3. That Defendant be required to identify any and all recipients of data obtained from the X platform;

4. Compensatory, statutory, and punitive damages, as permitted by law and in such amounts to be proven at trial;

5. Reasonable costs, including reasonable attorneys' fees;

6. Pre- and post-judgment interest, as permitted by law;

7. An accounting of Defendant's profits from its scraping activities and disgorgement

1 of those profits; and

2 8. Any other remedy to which Plaintiff X Corp., Inc. may be justly entitled.

3
4 Dated: November 14, 2023

Respectfully submitted,

5
6 **HAYNES & BOONE LLP**

7 By: /s/ Jason T. Lao

8 David H. Harper*

david.harper@haynesboone.com

9 Jason P. Bloom*

jason.bloom@haynesboone.com

2801 N. Harwood Street

Suite 2300

10 Dallas, Texas 75201

11 Telephone: (214) 651.5000

Telecopier: (214) 651.5940

12 * *Admitted Pro Hac Vice*

13 Jason T. Lao

jason.lao@haynesboone.com

14 Andrea Levenson

andrea.levenson@haynesboone.com

15 600 Anton Boulevard, Suite 700

Costa Mesa, California 92626

16 Telephone: (949) 202-3000

Facsimile: (949) 202-3001

17 *Attorneys for Plaintiff X Corp.*

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff hereby demands a trial by jury of all triable issues.

Dated: November 14, 2023

HAYNES AND BOONE LLP

By: /s/ Jason T. Lao
Jason T. Lao